EXHIBIT 3

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,851
	)	
U.S. Patent No. 7,418,504	)	Group Art Unit: 3992
	)	
Issued: August 26, 2008	)	Examiner: Roland Foster
	)	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	)	Confirmation No.: 1688

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PATENT OWNER'S RESPONSE TO OFFICE ACTION OF MARCH 1, 2012

(i) *Lendenmann*'s Cell Directory Service Used for "Returning the Network Address Corresponding to a Secure Domain Name" Does Not Disclose an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Office Action and the Request first assert that "by returning the network address corresponding to a secure domain name," the CDS provides "an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (OA at 11; Req. Ex. F-1 at 13.) This is incorrect.

Lendenmann discloses a conventional name service function for the CDS: "when given a name, CDS returns the network address of the named resource." (*Lendenmann* 21.) Rather than "comprising an indication that the domain name service system supports establishing a secure communication link," *Lendenmann* instead explains that the CDS merely provides server identification information to a client, as illustrated with Figure 15.

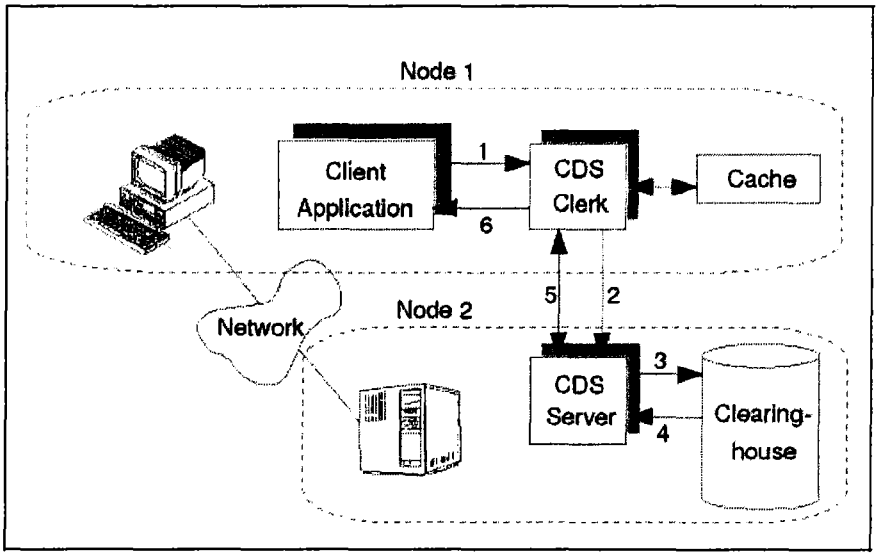

Figure 15. CDS Components Performing a CDS Look-up

(*Id.* at 29.) As *Lendenmann* explains, the CDS works as follows: (1) the client sends a lookup request to the CDS clerk; (2) the CDS clerk checks its cache and, not finding the name there, contacts the CDS server; (3) the CDS server checks to see if the name is in the clearinghouse; (4) the CDS server obtains the requested information if the name exists in the clearinghouse; (5) the CDS server then returns the information to the CDS clerk; and (6) the CDS clerk caches the information and passes the requested information to the client. (*Id.* at 29-30.) Thus, *Lendenmann* discloses a CDS lookup process that simply returns a name, taking no measures to provide any indication that the CDS supports establishing a secure communication link. (Keromytis Decl. ¶¶ 27-28.) Instead,

Lendenmann discloses a separate Security Service component that handles the aspects of any desired security measures. (*Lendenmann* 191-94.)

By simply returning server identification information to the client, the CDS disclosed in *Lendenmann* is consistent with a conventional domain name service system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. For instance, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host." ('504 patent 39:7-13.) In another example, the '504 patent identifies conventional domain name service systems that store public keys for different machines, allowing hosts to retrieve the keys and then proceed to communicate with the different machines to establish VPNs. (*Id.* at 39:34-42.) The '504 patent recognizes that such conventional domain name systems suffer from certain drawbacks and accordingly discloses various embodiments to address these problems, including "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, *id.* at 39:43-41:59; Keromytis Decl. ¶ 19.) Because the CDS disclosed in *Lendenmann* performs no functions beyond those that the '504 patent distinguishes as characterizing a conventional domain name service, one of ordinary skill in the art would not have understood *Lendenmann*'s CDS to comprise an indication that the domain name service system supports establishing a secure communication link, as recited in claim 1. (Keromytis Decl. ¶ 28.)

(ii) *Lendenmann*'s Cell Directory Service, "Integrated with the Security Services," Does Not Disclose an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Office Action and Request next assert that by only performing operations for users authorized by access control lists ("ACLs"), the CDS provides "an indication that the domain name service system supports establishing a secure communication link," as disclosed in claim 1. (OA at 11; Req. Ex. F-1 at 13-14.) This too is incorrect.

Lendenmann discloses that the Security Service plays a gatekeeper role to control access to the information in the CDS. For example, in response to a name request, "ACL management software examines the ACL entry associated with that name or principal name and grants or denies the [CDS] operation." (*Lendenmann* 34.) The Security Service's gatekeeping function, however, has no bearing on the operations of the alleged domain name service system, the CDS. (Keromytis Decl.

"wherein at least one of the plurality of domain names includes an indication that the domain name service system supports the establishment of a secure communication link." *Lendenmann* does not disclose these claim features.

The Request contends that DCE names containing a "sec" portion as an abbreviation for "security" discloses these claim features because this "sec" portion "indicates that the server is a security server." (Req. Ex. F-1 at 37-38.) But this is not what the claims recite. Claim 24, for example, recites that "at least one of the plurality of domain names comprises an indication that the *domain name service system* supports establishing a secure communication link" (emphasis added), as similarly recited by claim 48. The Request contends that the "sec" portion "indicates that the server is a security server," but the security status of a particular server indicates nothing regarding the capabilities of the alleged *domain name service system*, the CDS, and certainly would not indicate that *it* supports establishing a secure communication link.

Accordingly, *Lendenmann* does not disclose the features of claims 24 and 48, and the rejection of these claims should be withdrawn and their patentability confirmed.

f. Dependent Claims 2, 3, 6, 14, 15, 18-22, 25, 26, 28-30, 34, 35, 37-39, 42-46, 49, 50, 52-54, 58 and 59

Remaining claims 2, 3, 6, 14, 15, 18-22, 25, 26, 28-30, 34, 35, 37-39, 42-46, 49, 50, 52-54, 58 and 59 depend from one of independent claims 1 and 36, and include all of their features. Thus, *Lendenmann* does not anticipate any of these claims for at least the reasons discussed above in conjunction with independent claims 1 and 36. For the reasons set forth above, the rejection of these claims under 35 U.S.C. § 102 based on *Lendenmann* should be withdrawn and their patentability confirmed.

3. Rejection of Claims 1-6, 14-30, 33-54, and 57-60 Under 35 U.S.C. § 103(a) Based on *Lendenmann* (Issue 2)

The Office Action rejects claims 1-3, 5, 6, 14-30, 33-54, and 57-60 under 35 U.S.C. § 103(a) as being obvious over *Lendenmann*. (OA at 5.) However, the Request's and the Office Action's analysis of these claims is deficient. "The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious." M.P.E.P. § 2142. "[R]ejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Id.* (internal quotations omitted).

The Request and the Office Action fail to provide such a required articulated reasoning. Instead, the Request's and the Office Action's analysis in the § 103(a) rejection is *identical* to its

Aziz explains that "outside NS" 120 may receive a query for a host address located within domain 100 and may determine whether an SX record exists for that host name. (*Id.* at 9:49-53.) An SX record is a DNS resource record that "contains the identifier (e.g., name or address) of a 'secure exchanger,'" such as firewall 110. (*Id.* at 6:23-40.) If an SX record exists, then outside NS 120 may include the SX record in the response to the requester, which may also include the requested host address, if available. (*Id.* at 9:54-10:5.) *Aziz* also discloses that SIG (signature) and KEY resource records may be included in the response. (*Id.* at 9:35-41.)

Aziz also discloses a resolver 225, which is included in the "authorized client" 210 (*id.* at 8:5-50, Figs. 2A-2C), and receives a response to the query for a host address (*id.* at 10:39-41). If the response includes an SX record and the requested host address, then resolver 225 creates a tunnel map entry that provides the information "authorized client" 210 needs to encrypt messages to "inside host" 140. (*Id.* at 11:13-60.) Resolver 225 then returns the requested host address to an application 215, also located in "inside host" 140. (*Id.* at 11:55-60.) According to *Aziz*, "[t]his completes the execution" of the configuration process. (*Id.* at 11:60-62.)

2. Rejection of Claims 1, 2, 5-8, 14-25, 27, 28, 33-52, and 57-60 Under 35 U.S.C. § 102(b) Based on *Aziz* (Issue 9)

The Office Action rejects claims 1, 2, 5-8, 14-25, 27, 28, 33-52, and 57-60 under 35 U.S.C. § 102(b) based on *Aziz*. (OA at 11.) This rejection is deficient and should be withdrawn for at least the reasons discussed below.

a. Independent Claim 1

Aziz fails to disclose the combination of features recited in claim 1 for at least the reasons discussed below. Independent claim 1 recites, among other things, "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." The Request and the Office Action assert that four different features of *Aziz* disclose the recited indication. These assertions are incorrect because each asserted feature in *Aziz*, discussed in turn below, does not disclose a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link. Moreover, these features of *Aziz* disclose nothing more than a conventional domain name service system that is both recognized and distinguished by the '504 patent.

Before discussing the four different features of *Aziz* relied on by the Request, Patent Owner notes that Requester asserts in one portion of the Request that seemingly all of the elements shown in Fig. 1 of *Aziz* are included in the alleged domain name service system. (Req. Ex. F-2 at 5.) However, such an expansive reading is not consistent with the plain and ordinary meaning, and the

broadest reasonable interpretation, of the term "domain name service system." One of ordinary skill in the art would not have understood all of these elements in *Aziz* to be included in the recited domain name service system. (Keromytis Decl. ¶ 40.) Thus, this statement by the Requester is not reasonable. Moreover, the Request, when considered as a whole and, especially with regard to the analysis of the element that the Request identifies as [1.5], appears to assume that NS 120 is the recited domain name service system. (*See, e.g.*, Req. Ex. F-2 at 7-11, relying on resource records such as SX, KEY, and SIG resource records that are stored in *NS 120* as being the recited "indication.")

Further, the Office Action takes the position that the NS 120 of *Aziz* is the recited domain name service system. For example, the Office Action asserts that "[r]egarding the limitation 'domain name service [system] configured for connection [sic] to a communication network' . . . [s]ee also Fig. 1, reproduced below which illustrates the *outside name server 120* (NDS) [sic] connected to public network 190." (OA at 13, emphasis added.) The Office Action continues: "[r]egarding the limitation to provide an 'indication that the domain name service [system] supports establishing a secure communication[] link,' *Aziz* describes configuring the DNS to respond to requests with a special record that includes information needed for secure communications . . . . Thus, the presence of SX records in the response from the *DNS* (*NS 120*) provides an *indication that the DNS* [supports] establishing a secure communication link." (*Id.* at 15, emphases added.) Because the Request's assertion that essentially all of the elements in Fig. 1 of *Aziz* constitute a domain name service system is unreasonable and is belied by other portions of its analysis, and because the Office Action ultimately takes the position that the NS 120 is the recited domain name service system, Patent Owner's remarks below address the rejections in view of *Aziz* based on the Office Action's position that the NS 120 is the recited domain name service system.

(i) *Aziz*'s SX Records Do Not Disclose an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

First, the Request and the Office Action assert that providing "SX records in the response from the DNS (NS 120) provides an indication that the DNS [supports] establishing a secure communication link." (*Id.*; *see also* Req. Ex. F-2 at 7-8.) This is incorrect. The SX record in *Aziz* is not an indication that the alleged domain name service system (NS 120) supports establishing a secure communication link. Instead, the SX record merely "contains the identifier (e.g., name or address) of a 'secure exchanger' [i.e., firewall 110] associated with the owner of the record." (*Aziz* 6:27-38.) Thus, the SX record includes the name or address of firewall 110, which is separate from

the alleged domain name service system, NS 120. (Keromytis Decl. ¶ 42; *see also Aziz* Fig. 1, showing NS 120 separate from firewall 110.) While including the name or address of firewall 110, the SX record includes no indication about the capabilities of the alleged domain name service system itself or about the capabilities of firewall 110, and certainly does not include an indication that the domain name service system supports establishing a secure communication link, as recited in claim 1. (Keromytis Decl. ¶ 42.)

Indeed, returning an SX record with the name or address of firewall 110 in *Aziz* is a feature of a conventional domain name service system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:7-42; Keromytis Decl. ¶ 43.) As discussed, the '504 patent indicates that a conventional domain name service system merely returns an IP address or public key that was requested of it. (Keromytis Decl. ¶ 43.) For instance, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that *returns the IP address* of a requested computer or host. For example, when a computer user types in the web name 'Yahoo.com,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . ." ('504 patent 39:7-13, emphasis added; Keromytis Decl. ¶ 43; *see also* '504 patent 39:14-42.) Similar to the conventional domain name systems described by the '504 patent, the NS 120 in *Aziz* merely returns an SX resource record requested for a particular domain name that includes the *name or address* of a secure exchanger associated with that domain name. (*See, e.g.*, *Aziz* 9:49-56, 6:27-38; Keromytis Decl. ¶¶ 42-43.)

The '504 patent recognizes that such conventional domain name systems suffer from certain drawbacks and thus discloses embodiments that address them, including "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:43-41:61; Keromytis Decl. ¶ 19.) And since returning a name or address is a feature of a conventional domain name server of the type distinguished by the '504 patent, one of ordinary skill in the art would not have understood *Aziz*'s SX record to disclose an indication that the domain name service system supports establishing a secure communication link, as recited in claim 1. (Keromytis Decl. ¶¶ 42-43.)

(ii) *Aziz*'s KEY and SIG Records Do Not Disclose an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Request and the Office Action assert that *Aziz* discloses a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link "by providing secure DNS service." (OA at 16; Req. Ex. F-2 at 9.) The explanation in the Request and the summary in the Office Action make clear that when referring to "providing secure DNS service," the Request and the Office Action are asserting that the SIG and KEY resource records in *Aziz* are the recited "indication." (*Id.* at 9-10; *see also* OA at 15, stating that "*Aziz* describes automatically adding the KEY and SIG records, which also provides 'an indication' . . . .") This is incorrect because the KEY and SIG records do not provide an indication that *the alleged domain name service system* (*NS 120*) supports establishing a secure communication link. Instead, KEY and SIG records provided in *Aziz* correspond to resource records. (*Aziz* 9:35-41, stating that whenever a resource record is added to a response, the "appropriate SIG and KEY records are also added (i.e., one SIG record for each record type and record owner combination and the KEY record used to generate the SIG record)"; Keromytis Decl. ¶ 45.) But these resource records returned in *Aziz* are A records and SX records that correspond to the inside host 140 and the firewall 110, respectively, which are both separate from the alleged domain name service system, NS 120. (*Aziz* 9:40-67, Fig. 1; Keromytis Decl. ¶ 45.) Thus, these KEY or SIG resource records in *Aziz* include no indication about the capabilities of *the alleged domain name service system itself*, and certainly do not include an indication that the domain name service system supports establishing a secure communication link, as recited in claim 1. (Keromytis Decl. ¶ 45.)

Moreover, returning KEY and SIG resource records in *Aziz* is consistent with a conventional domain name system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*,'504 patent 39:7-42; Keromytis Decl. ¶ 43, 45.) As discussed, the '504 patent indicates that a conventional domain name system merely stores *public keys* of different machines so that hosts can request and receive those public keys from the domain name service system. ('504 patent 39:34-42; Keromytis Decl. ¶¶ 19, 45.) The '504 patent explains that an example of such a conventional system is disclosed in RFC 2535, which describes the very same KEY and SIG resource records disclosed in *Aziz*. ('504 patent 39:40-42; *see also* Ex. A-6 at 10-23, disclosing the KEY and SIG resource record types.) Thus, the NS 120 in *Aziz* merely returning KEY and SIG resource records is an aspect of a conventional system that the '504

patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:7-42; Keromytis Decl. ¶¶ 19, 45.) Accordingly, the KEY and SIG resource records also are not an indication that the domain name service system supports establishing a secure communication link.

(iii) *Aziz*'s "Information Used for Secure Communications with Protected Hosts" Does Not Disclose an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Request and the Office Action also assert that *Aziz* discloses the recited indication "by providing the information needed for secure communications between a client and a protected host." (OA at 16; Req. Ex. F-2 at 8-9.) To support this assertion, the Request cites two portions of *Aziz*. Neither portion of *Aziz* discloses a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link.

The first portion of *Aziz* cited by the Request states that "[t]he data in the SX record is used by a program called a resolver to update information used by a client for secure communications with protected hosts." (*Aziz* 6:57-60.) However, as discussed above, "the data in the SX record" is the name or address of the secure exchanger. (*Id.* at 6:27-38.) And, as discussed above, merely providing the SX record with this name or address in *Aziz* does not disclose an indication that the domain name service system supports establishing a secure communication link and is a conventional feature of a domain name service system that the '504 patent recognizes and distinguishes.

The second portion of *Aziz* cited by the Request states that the resolver "update[s] a data structure on a client containing information used for secure communications with protected hosts .... Such a data structure comprises data sets whose fields typically contain 'tunnel information' (e.g., destination and secure exchanger addresses) and related cryptographic data (e.g., secure exchanger's key or algorithm)." (*Id.* at 7:28-36.) The "data structure on a client containing information used for secure communications" does not disclose a *domain name service system* configured to comprise an indication that the domain name service system supports establishing a secure communication link for two reasons.

First, *Aziz* clearly discloses that "the data structure" is "on a client," which is separate from the alleged domain name service system, NS 120. (*Id.* at 7:30, Fig. 1.) Thus, "the data structure" does not disclose a *domain name service system* configured to comprise any indication. (Keromytis Decl. ¶ 48.) Second, *Aziz* discloses that the data structure includes "destination and secure exchanger

Req. Ex. F-2 at 11-13, 41.) But authenticating data in a DNS resource record does not disclose "authenticat[ing] the query [for a network address]," as recited in claim 5. (Keromytis Decl. ¶ 64.) In fact, one of ordinary skill in the art would have understood that a DNS resource record is generally not a query for a network address. (*Id.*) Moreover, merely disclosing that the SIG resource record "*can be used* to authenticate data" does not disclose that "*the domain name service system* is configured to authenticate" anything. (*Id.*) In fact, *Aziz* does not disclose that the alleged domain name service system (NS 120) authenticates queries with the SIG resource record. (*Id.*)

The second portion of *Aziz* relied upon by the Request describes authentication in general terms, stating that "[a]uthentication means that a host is assured that the message is from the client that the message claims," and then lists several standard cryptographic methods. (*Aziz* 3:22-29; *see* Req. Ex. F-2 at 11-13, 28-29, 41.) General statements about the meaning of authentication also do not disclose that "the domain name service system is configured to authenticate the query using a cryptographic technique," as recited in claim 5. (Keromytis Decl. ¶ 65.)

Thus, *Aziz* has not been shown to disclose that "the domain name service system is configured to authenticate the query [for a network address] using a cryptographic technique," as recited in claim 5 and similarly recited in claims 23 and 47. Accordingly, Patent Owner requests that the rejection of claims 5, 23, and 47 under 35 U.S.C. § 102 be withdrawn, and the patentability of claims 5, 23, and 47 be confirmed.

d. Dependent Claim 8

Dependent claim 8 depends from independent claim 1 and includes all of its features. Thus, *Aziz* does not anticipate claim 8, and the rejection of this claim should be withdrawn, at least for the reasons discussed above in connection with independent claim 1. Dependent claim 8 also distinguishes over *Aziz* for additional reasons. For example, dependent claim 8 also recites that "the domain name service system is connectable to a virtual private network through the communication network."

The Request cites a portion of *Aziz* that describes inside NS 130 inside a protected zone 180 and asserts that "[h]aving the 'inside NS [130]' (inside Name Server) within the 'protected zone'. . . shows the domain name service system is connectable to a virtual private network . . . ." (Req. Ex. F-2 at 15.) As discussed, however, outside NS 120, and not inside NS 130 of *Aziz*, is the alleged domain name service system. But *Aziz* does not disclose that NS 120, the alleged domain name service system, is connectable to a virtual private network. Because *Aziz* does not disclose that the alleged domain name service system is connectable to a virtual private network, *Aziz* does not

3. Rejection of Claims 1-4, 6, 8-10, 12-19, 22, 24-30, 33, 34, 36-43, 46, 48-54, and 57-60 Under 35 U.S.C. § 103(a) Based on *Kiuchi* in View of *Pfaffenberger* (Issue 16)

The Office Action rejects claims 1-4, 6, 8-10, 12-19, 22, 24-30, 33, 34, 36-43, 46, 48-54, and 57-60 under 35 U.S.C. § 103(a) over *Kiuchi* in view of *Pfaffenberger*. (OA at 16.) This rejection is deficient and should be withdrawn for at least the reasons discussed below.

a. Independent Claim 1

Kiuchi fails to disclose the combination of features recited in claim 1 for at least the reasons discussed below. Independent claim 1 recites, among other things, "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." The Request and the Office Action assert that two different features of *Kiuchi* disclose the recited indication. The Request and the Office Action are incorrect because each asserted feature in *Kiuchi*, discussed in turn below, does not disclose a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link. Moreover, these features of *Kiuchi* are nothing more than features of a conventional domain name service system recognized and distinguished by the '504 patent.

(i) The C-HTTP Name Server Returning the Public Key of the Server-Side Proxy Is Not an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

Incorporating portions of the Request by reference, the Office Action contends that "[t]he sending of the 'public key' [of the server-side proxy] is an indication that the domain name service [system] (C-HTTP name server) supports the establishment of [a] subsequent, secure communication link . . . ." (OA at 18; *see also* Req. Ex. F-3 at 11, quoting *Kiuchi* 65.) This is incorrect.

The public key of the server-side proxy returned by *Kiuchi*'s C-HTTP name server is not an indication that the alleged *domain name service system*, the C-HTTP name server, supports establishing a secure communication link. The client-side proxy uses the public key of the server-side proxy to send an encrypted connection request to the server-side proxy. (*Kiuchi* 65; Keromytis Decl. ¶ 56.) Thus, the public key corresponds to the server-side proxy, which is separate from the alleged domain name service system, the C-HTTP name server. (Keromytis Decl. ¶ 56.) The public key of the server-side proxy in *Kiuchi* includes no indication about the capabilities of the *C-HTTP name server itself*, and certainly does not include an indication that the C-HTTP name server supports establishing a secure communication link. (*Id.*)

Moreover, the C-HTTP name server in *Kiuchi* returning a public key of a server-side proxy is consistent with a conventional domain name service system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:7-42; Keromytis Decl. ¶ 57.) As discussed, the '504 patent indicates that a conventional domain name service system stores *public keys* of different machines so that hosts can request and receive those public keys from the domain name service system. ('504 patent 39:34-42; Keromytis Decl. ¶ 19, 57.) Like the conventional domain name service system described in the '504 patent, the C-HTTP name server of *Kiuchi* returns the public key of a server-side proxy when provided with the host URL for the server-side proxy. (*Kiuchi* 65; Keromytis Decl. ¶ 57.) Thus, the C-HTTP name server returning the public key of the server-side proxy is an aspect of a conventional domain name system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:7-42; Keromytis Decl. ¶¶ 56-57.)

Accordingly, the C-HTTP name server of *Kiuchi* returning a public key of a server-side proxy does not disclose a domain name service system configured to comprise an indication that the *domain name service system* supports establishing a secure communication link, as claimed.

(ii) The C-HTTP Name Server Returning the IP Address of the Server-Side Proxy Is Not an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Request also contends that the C-HTTP name server returning the IP address of the server-side proxy is an indication that the alleged domain name service system, the C-HTTP name server, supports establishing a secure communication link. (Req. at 24; Req. Ex. F-3 at 11, quoting *Kiuchi* 65.) However, it appears that the Office Action does not adopt the Request's position, as the Office Action only contends that the public key of the server-side proxy in *Kiuchi* is the claimed indication. (*See* OA at 18.) Thus, Patent Owner does not believe the Request's contention—that the C-HTTP name server returning the IP address of the server-side proxy is an indication that the C-HTTP name server supports establishing a secure communication link—is part of the rejection. Nonetheless, out of an abundance of caution, the Request's contention is addressed below.

Like returning the public key, the C-HTTP name server in *Kiuchi* returning the IP address of the server-side proxy is not an indication that the alleged *domain name service system*, the C-HTTP

name server, supports establishing a secure communication link. The IP address is for the server-side proxy, which is separate from the alleged domain name service system, the C-HTTP name server. (Keromytis Decl. ¶ 58.) Moreover, the IP address includes no indication about the capabilities of the C-HTTP name server itself, and certainly does not include an indication that the C-HTTP name server supports establishing a secure communication link. (*Id.*) It is just the address the C-HTTP name server returns when it receives a corresponding URL from the client-side proxy. (*See Kiuchi* 65; Keromytis Decl. ¶ 58.)

Like returning a public key, the C-HTTP name server returning the IP address of the server-side proxy in *Kiuchi* is a feature of a conventional domain name system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:7-42; Keromytis Decl. ¶ 19, 58.) As discussed, the '504 patent indicates that a conventional domain name service system merely returns an IP address or public key that was requested of it. (Keromytis Decl. ¶ 19.) For instance, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that *returns the IP address* of a requested computer or host. For example, when a computer user types in the web name 'Yahoo.com,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . ." ('504 patent 39:7-13, emphasis added; Keromytis Decl. ¶ 19; *see also* '504 patent 39:14-42.) Similar to the conventional domain name systems described by the '504 patent, the C-HTTP name server in *Kiuchi* returns an IP address corresponding to a provided URL. (*See Kiuchi* 65; Keromytis Decl. ¶ 58.)

Accordingly, the C-HTTP name server of *Kiuchi* returning an IP address of a server-side proxy does not disclose a domain name service system configured to comprise an indication that the *domain name service system* supports establishing a secure communication link, as claimed.

For the reasons provided above, *Kiuchi* has not been shown to disclose a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link, as recited in claim 1.

(iii) *Pfaffenberger* Does Not Remedy the Deficiencies of *Kiuchi*

In addition to alleging that *Kiuchi* discloses the claimed indication, the Request and the Office Action further contend that *Pfaffenberger* discloses the claimed indication, and that it would have been obvious to combine *Pfaffenberger* with *Kiuchi* to arrive at this subject matter of independent claim 1. (*See* OA at 18; Req. at 24-26; Req. Ex. F-3 at 2-3, 11-12.) The Request and

b. Independent Claims 36 and 60

Independent claims 36 and 60 include recitations similar to those described above with respect to claim 1. For example, claim 36 recites "instructions executable in a domain name service system, the instructions comprising code for: . . . supporting an indication that the domain name service system supports establishing a secure communication link." And claim 60 recites, for example, "the domain name service system comprising an indication that the domain name service system supports establishing a secure communication link." And the Request incorporates by reference its analysis for independent claim 1 when addressing these features of independent claims 36 and 60. (*See* Req. Ex. F-3 at 41, 48-49.) Thus, for reasons similar to those discussed above in connection with independent claim 1, *Kiuchi* and *Pfaffenberger* would not have rendered obvious the subject matter of independent claims 36 and 60. Accordingly, Patent Owner requests that the rejection of claims 36 and 60 under 35 U.S.C. § 103 be withdrawn, and that the patentability of the claims be confirmed.

c. Dependent Claims 8, 9, 10, 12, and 13

Dependent claim 8 depends from independent claim 1 and includes all of its features. Thus, the combination of *Kiuchi* and *Pfaffenberger* does not render obvious claim 8, and the rejection of this claim should be withdrawn, at least for the reasons discussed above in connection with independent claim 1. Claim 8 also distinguishes over the combination for additional reasons. For example, claim 8 recites that "the domain name service system is connectable to a virtual private network through the communication network." Claims 9, 10, 12, and 13 also include these features because they depend from claim 8. Thus, the combination of *Kiuchi* and *Pfaffenberger* also does not disclose or suggest these additional features.

The Request contends that the C-HTTP connection in *Kiuchi* corresponds to the virtual private network recited in claim 8. (*See, e.g.*, Req. Ex. F-3 at 14-16.) One of ordinary skill in the art would not have viewed the C-HTTP connection in *Kiuchi* as a virtual private network in the context of the '504 patent.

One of ordinary skill, having read the '504 patent, would have understood a virtual private network, as recited in claims 8-13, to be a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers. (Keromytis Decl. ¶ 77.) For instance, suppose two computers A and B reside on a public network and two computers X and Y reside on a private network. (*Id.*) If A establishes a virtual private network with X and Y's network to address data to X, and B separately establishes a virtual private

network with X and Y's network to address data to Y, then A would nevertheless be able to securely address data to B, X, and Y without additional setup. (*Id.*) This is true because A, B, X, and Y would all be part of the same virtual private network. (*Id.*)[3] *Kiuchi* fails to disclose such a virtual private network. (*Id.*)

But *Kiuchi*'s C-HTTP connection is very different from the claimed virtual private network. (*Id.* ¶ 78.) In *Kiuchi*'s C-HTTP system, a specific point-to-point connection is established each time a computer is to communicate with another computer using C-HTTP. (*Id.*) For instance, suppose, according to *Kiuchi*, a computer A (i.e., user agent or client-side proxy) establishes a C-HTTP session with a computer X (i.e., origin server or server-side proxy) in the closed network, and a computer B (i.e., user agent or client-side proxy) separately establishes a C-HTTP session with a computer Y (i.e., origin server or client-side proxy) in the same closed network. (*Id.*) In this case, computer A would be unable to access computer Y via a C-HTTP connection without first ending the existing C-HTTP session with computer X and again engaging in the C-HTTP setup process described above to establish a C-HTTP session with computer Y. (*Kiuchi* 65-66; Keromytis Decl. ¶ 78.) Similarly, computer B would be unable to communicate with computer X using C-HTTP without ending its session with computer Y and again completing the setup process to establish a new C-HTTP session with computer X. (Keromytis Decl. ¶ 78.) This is because *Kiuchi*'s C-HTTP connection is a point-to-point connection in which "[t]he [C-HTTP] session is finished when the client accesses another C-HTTP server." (*Kiuchi* 65; Keromytis Decl. ¶ 78.) In fact, Figure (b) of *Kiuchi* shows that C-HTTP connections to different servers in the closed network have distinct connection IDs:

b. The HTML document rewritten and forwarded to a use agent by the client-side proxy. The string, "6zdDfldfcZLj8V!i", attached to the end of the URLs is a connection ID

```
<TITLE>SAMPLE</TITLE>
<BODY>
<A HREF =
"http://server.in.current.connection/sample.html=@
=6zdDfldfcZLj8V!i">
Please click here.</A>
<A HREF =
"http://another.server.in.closed.network/=@=6zdDfl
dfcZLj8V!i">
Another server.</A>
</BODY>
```

[3] This view of "virtual private network" is supported by the interpretation of the term offered by another expert in the reexamination proceedings for other patents in the Munger patent family. (*See* Decls. of Jason Nieh, Ph.D., in control nos. 95/001,269 and 95/001,270.)

(*Kiuchi* 66; Keromytis Decl. ¶ 78.) And, as discussed, the server-side proxy generates the connection ID for a given C-HTTP connection during the above-described C-HTTP session setup process. (Keromytis Decl. ¶ 78.) This confirms that a C-HTTP connection is of a point-to-point nature and requires a new C-HTTP setup process each time a computer is to communicate with another computer using C-HTTP. (*Id.*)

In light of the additional setup required each time a client communicates with a different server using C-HTTP, one of ordinary skill in the art would have understood *Kiuchi*'s C-HTTP connection as a point-to-point connection rather than the claimed virtual private network. (*Id.* at 79.) Indeed, for at least this reason, one of ordinary skill in the art would not have understood computers connected via C-HTTP to be part of a virtual private network at all. (*Id.*)

Moreover, claim 8 recites that "*the domain name service system* is connectable to a virtual private network through the communication network" (emphasis added). The Request points to the C-HTTP communication between *the client-side proxy and the server-side proxy* as the claimed virtual private network. (Req. Ex. F-3 at 15, citing *Kiuchi* 64.) As explained by *Kiuchi*, "[o]nce the connection [between the proxies] is established, a client-side proxy forwards HTTP/1.0 requests from the user agent in encrypted form using C-HTTP format." (*Kiuchi* 66.) But this C-HTTP communication between the *proxies*, the alleged virtual private network, does not include the alleged *domain name service system*, the C-HTTP name server. (Keromytis Decl. ¶ 80.) Indeed, the alleged virtual private network in *Kiuchi* is not used for communication until after the proxies have already communicated with the C-HTTP name server to obtain each other's public keys and IP addresses. (*See id.* at 65-66; Keromytis Decl. ¶ 80.) Thus, the alleged domain name service system in *Kiuchi*, the C-HTTP name server, is not connectable to the alleged virtual private network, the C-HTTP communication between the proxies. (Keromytis Decl. ¶ 80.)

For the above reasons, *Kiuchi* fails to disclose the features of claims 8-13. Moreover, *Pfaffenberger* does not remedy the deficiencies of *Kiuchi* at least because *Pfaffenberger* also fails to disclose a domain name service system connectable to a virtual private network, as required by claims 8-10, 12, and 13. Nor does the Office Action or Request rely on *Pfaffenberger* for such disclosure. Accordingly, the combination fails to render obvious the features of claims 8-10, 12, and 13, and the rejection of these claims under 35 U.S.C. § 103(a) over *Kiuchi* in view of *Pfaffenberger* should be withdrawn and the claims should be confirmed.

d. Dependent Claim 10

Dependent claim 10 depends from independent claim 1 via claim 8, and thus includes all of the features of these claims. Accordingly, the combination of *Kiuchi* and *Pfaffenberger* does not render obvious claim 10, and the rejection of this claim should be withdrawn, at least for the reasons discussed above in connection with claims 1 and 8. Claim 10 also distinguishes over the combination for additional reasons. For example, claim 10 recites that "the virtual private network is based on inserting into each data packet communicated over a secure communication link one or more data values that vary according to a pseudo-random sequence." The combination of *Kiuchi* and *Pfaffenberger* also does not render obvious these additional features.

The Request contends that *Kiuchi*'s disclosure of inserting "[r]andom bytes" "every fourth byte of the request and response before encryption in order to avoid the same encrypted requests or responses being repeated" discloses the above features of claim 10. (Req. Ex. F-3 at 17, citing *Kiuchi* 72.) This is incorrect at least because the random bytes are not inserted into packets of the alleged virtual private network in *Kiuchi, the C-HTTP connection between the proxies*. (Keromytis Decl. ¶ 81.)

The passage of *Kiuchi* cited in the Office Action is from Appendix 2A of *Kiuchi*, entitled "The summary of C-HTTP name server protocol." (*Kiuchi* 72.) As indicated by its title, Appendix 2A relates to name requests/responses *between the proxies and the C-HTTP name server*. (*Id.*; Keromytis Decl. ¶ 82.) In the cited passage, *Kiuchi* explains that random bytes are inserted into *name requests/responses between the proxies and the C-HTTP name server*. (*Kiuchi* 72; Keromytis Decl. ¶ 82.) But, as discussed above in connection with claim 8 from which claim 10 depends, the Request takes the position that the encrypted C-HTTP communication between the client-side proxy and server-side proxy, not the communication of name requests/responses between the proxies and the C-HTTP name server, corresponds to the claimed virtual private network. Thus, these random bytes are not inserted into data packets of the alleged virtual private network but into separate name requests/responses between the proxies and the C-HTTP name server. Thus, *Kiuchi* does not disclose that the alleged *virtual private network* is based on inserting into each data packet communicated over a secure communication link one or more data values that vary according to a pseudo-random sequence, as claimed.

In addition, the Request's analysis of claim 10 is deficient because it improperly relies on different components of *Kiuchi* for the same claimed element. But "[t]he key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention

would have been obvious." M.P.E.P. § 2142. This involves, among other things, considering all of the elements of the claim. *Id.* § 2143.03. By relying on different components of *Kiuchi* for the same element of claim 10, the Request has failed to provide a clear articulation of the reasons why the claimed invention would have been obvious.

In particular, the Request and Office Action rely on one alleged virtual private network (the encrypted C-HTTP communication between the client-side proxy and server-side proxy) for claim 8 and on another alleged virtual private network (the separate name requests/responses between the proxies and the C-HTTP name server) for claim 10. But claim 10 depends from claim 8 and refers to the same "virtual private network." Because of this inconsistency in the Request's analysis, the Request has not demonstrated, or even properly alleged, that *Kiuchi* discloses or suggests that the alleged *virtual private network* is based on inserting into each data packet communicated over a secure communication link one or more data values that vary according to a pseudo-random sequence, as recited in claim 10.

Moreover, *Kiuchi* discloses that these random bytes are inserted into *C-HTTP name requests and responses*. (*See Kiuchi* 72; Keromytis Decl. ¶ 83.) *Kiuchi* does not disclose that the random bytes are inserted into *each data packet*. Accordingly, even if the random bytes are viewed as the claimed "one or more data values that vary according to a pseudo-random sequence," *Kiuchi* still does not disclose that they are inserted into *each data packet*, as claimed. One of ordinary skill in the art would not have considered *Kiuchi*'s C-HTTP name requests and responses, which are application layer communications, to be data packets. (Keromytis Decl. ¶ 83.)

For the above reasons, *Kiuchi* fails to disclose the features of claim 10. Moreover, *Pfaffenberger* does not remedy the above-noted deficiencies of *Kiuchi* at least because *Pfaffenberger* also fails to disclose a virtual private network based on inserting into each data packet communicated over a secure communication link one or more data values that vary according to a pseudo-random sequence, as recited in claim 10. Nor does the Office Action or Request rely on *Pfaffenberger* for such disclosure. Accordingly, the combination fails to render obvious the features of claim 10, and the rejection of this claim under 35 U.S.C. § 103(a) over *Kiuchi* in view of *Pfaffenberger* should be withdrawn and the claim should be confirmed.

e. Dependent Claim 12

Dependent claim 12 depends from independent claim 1 via claim 8, and thus includes all of the features of these claims. Accordingly, the combination of *Kiuchi* and *Pfaffenberger* does not render obvious claim 12, and the rejection of this claim should be withdrawn, at least for the reasons

discussed above in connection with claims 1 and 8. Claim 12 also distinguishes over the combination for additional reasons. For example, claim 12 recites that "the virtual private network is based on comparing a value in each data packet transmitted between a first device and a second device to a moving window of valid values." The combination of *Kiuchi* and *Pfaffenberger* also does not disclose or render obvious these additional features.

The Request and the Office Action allege that the Nonce values contained in the headers of *Kiuchi*'s C-HTTP requests and responses constitute the claimed "value in each data packet." (OA at 18; Req. Ex. F-3 at 17-19.) Specifically, they allege that, "[i]n the Examples of C-HTTP communication found in Appendix 3, it can be seen that the 'Request-Nonce value' is incremented, moving from '8abd853f' in Example c., to '8abd8540' in Example g., to '8abd8541' in Example i." (*Id.* at 18.) According to *Kiuchi*, Example c. is a "Request for connection to the server-side proxy," Example g. is "Sending C-HTTP requests to the server-side proxy," and Example i. is a "Request for closing the connection." (*Kiuchi* 74.) At best, the Request has just shown that different requests contain different Nonce values.[4] (Keromytis Decl. ¶ 85.) The Request has not shown, and *Kiuchi* does not disclose, however, that these Nonce values are compared to a moving window of valid values, as recited in claim 12. *Kiuchi* just mentions that the "[r]eplay attacks are blocked by *checking* values of the Request-Nonce header field." (*Kiuchi.* at 65, emphasis added.) But *Kiuchi* does not explain *how* the values of the Nonce header field are checked, and certainly does not teach that they are checked by comparing them to a moving window of valid values. Further, there are many ways that the values of the Nonce header field could be checked without comparing them to a moving window of valid values. (Keromytis Decl. ¶ 85.) Thus, this feature is neither disclosed by, nor inherent in, *Kiuchi.*

In addition, as discussed, *Kiuchi* teaches that C-HTTP *requests* and *responses* contain a Nonce value in a Nonce header field. (*See Kiuchi* 65, 71; Keromytis Decl. ¶ 87.) But *Kiuchi* does not teach that Nonce values are inserted into *each data packet.* Accordingly, even if the Nonce values were compared to a moving window of valid values (which they are not), *Kiuchi* still does not disclose that the virtual private network is based on comparing a value in *each data packet* transmitted between the first computer and the second computer to a moving window of valid values, as claimed. One of ordinary skill in the art would not have considered *Kiuchi*'s C-HTTP requests and responses, which are application layer requests, to be data packets. (Keromytis Decl. ¶ 87.)

[4] Indeed, in secure communications, a nonce is a unique, arbitrary number used only once to identify a particular communication.

For the above reasons, *Kiuchi* fails to disclose the features of claim 12. Moreover, *Pfaffenberger* does not remedy the deficiencies of *Kiuchi* at least because *Pfaffenberger* also fails to disclose that "the virtual private network is based on comparing a value in each data packet transmitted between a first device and a second device to a moving window of valid values," as recited in claim 12. Nor does the Office Action or Request rely on *Pfaffenberger* for such disclosure. Accordingly, the combination fails to render obvious the features of claim 12, and the rejection of this claim under 35 U.S.C. § 103(a) over *Kiuchi* in view of *Pfaffenberger* should be withdrawn and the claim should be confirmed.

f. Dependent Claim 13

Dependent claim 13 depends from independent claim 1 via claim 8, and thus includes all of the features of these claims. Accordingly, the combination of *Kiuchi* and *Pfaffenberger* does not render obvious claim 13, and the rejection of this claim should be withdrawn, at least for the reasons discussed above in connection with claims 1 and 8. Claim 13 also distinguishes over the combination for additional reasons. For example, claim 13 recites that "the virtual private network is based on a comparison of a discriminator field in a header of each data packet to a table of valid discriminator fields maintained for a first device." The combination of *Kiuchi* and *Pfaffenberger* also does not disclose or render obvious these additional features.

The Request and the Office Action contend that "*Kiuchi* teaches that the virtual private network . . . is based on a comparison of a connection ID field in the header of a request to a table of valid discriminator fields" because the connection ID is compared to a current connection table or list. (OA at 18; Req. Ex. F-3 at 20-21.) As pointed out in the Request, *Kiuchi* explains that the alleged discriminator field, a connection ID, is included in certain *C-HTTP requests*. But, again, *Kiuchi* does not teach that a connection ID is in a header of *each data packet*, as claimed. One of ordinary skill in the art would not have considered *Kiuchi*'s C-HTTP requests, which are application layer requests, to be data packets. (Keromytis Decl. ¶ 87.)

For the above reasons, *Kiuchi* fails to disclose the features of claim 13. Moreover, *Pfaffenberger* does not remedy the deficiencies of *Kiuchi* at least because *Pfaffenberger* also fails to disclose that "the virtual private network is based on a comparison of a discriminator field in a header of each data packet to a table of valid discriminator fields maintained for a first device," as recited in claim 13. Nor does the Office Action or Request rely on *Pfaffenberger* for such disclosure. Accordingly, the combination fails to render obvious the features of claim 13, and the rejection of

this claim under 35 U.S.C. § 103(a) over *Kiuchi* in view of *Pfaffenberger* should be withdrawn and the claim should be confirmed.

g. Dependent Claims 17 and 41

Claims 17 and 41 depend from claims 1 and 36, respectively. As discussed above with regard to independent claims 1 and 36, the combination of *Kiuchi* in view of *Pfaffenberger* does not disclose or suggest the recited domain name service system that is configured to comprise an indication that the domain name service system supports establishing a secure communication link. Because the combination does not disclose or suggest such a domain name service system, it also does not disclose or suggest that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link, as recited in claim 17 and similarly recited in claim 41.

The Request incorporates by reference its analysis of independent claim 1 with respect to these features of claims 17 and 41. (*See id.* at 26, 43.) Accordingly, for reasons similar to those discussed above as to why those alleged features of *Kiuchi* and *Pfaffenberger* do not disclose or suggest a domain name service system that is configured to comprise an indication that the domain name service system supports establishing a secure communication link, those features of *Kiuchi* and *Pfaffenberger* also do not disclose or suggest the recited features of claims 17 and 41. Accordingly, the combination of *Kiuchi* and *Pfaffenberger* fails to render obvious the features of claims 17 and 41, and the rejection of these claims under 35 U.S.C. § 103(a) over *Kiuchi* in view of *Pfaffenberger* should be withdrawn and the claims should be confirmed.

h. Dependent Claims 24 and 48

Dependent claims 24 and 48 depend from independent claims 1 and 36, respectively, and thus include all of the features of these claims. Accordingly, the combination of *Kiuchi* and *Pfaffenberger* does not render obvious claims 24 and 48, and the rejection of these claims should be withdrawn, at least for the reasons discussed above in connection with independent claims 1 and 36. Claims 24 and 48 also distinguish over the combination for additional reasons. For example, claim 24 recites that "at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link," and claim 48 similarly recites that "at least one of the plurality of domain names includes an indication that the domain name service system supports the establishment of a secure communication link."

The Request contends that *Kiuchi* discloses these features because "*Kiuchi* provides example domain names that expressly indicate that the server is included within the secure C-HTTP closed

26. Moreover, *Pfaffenberger* does not remedy the deficiencies of *Kiuchi* at least because *Pfaffenberger* also fails to disclose that at least one of the plurality of domain names enables establishment of a secure communication link, as recited in claim 26. Nor does the Office Action or Request rely on *Pfaffenberger* for such disclosure. Accordingly, the rejection of claim 26 in view of *Kiuchi* and *Pfaffenberger* should be withdrawn and the claim should be confirmed.

j. Dependent Claim 27

Dependent claim 27 recites that "the domain name service system is configured to enable establishment of a secure communication link between a first location and a second location transparently to a user at the first location." *Kiuchi* and *Pfaffenberger*, alone or in combination, have not been shown to disclose or suggest this feature.

With respect to this feature of the claim, the Request contends that "*Kiuchi* teaches that the secure C-HTTP closed network is designed to include a proxy server at each participating hospital" and that "the client-side proxy that processes a request for a user is located at the same institution as the user." (Req. Ex. F-3 at 32-33, citing *Kiuchi* 65.) However, that *Kiuchi*'s C-HTTP closed network allegedly includes proxies that process a request for a user does not demonstrate anything about what the alleged *domain name service system*, the C-HTTP name server, is configured to do. And it certainly does not disclose that the *C-HTTP name server* is configured to enable establishment of a secure communication link between a first location and a second location transparently to a user at the first location, as recited in claim 26.

Accordingly, the Request has not demonstrated that *Kiuchi* discloses that "the *domain name service system* is configured to enable establishment of a secure communication link between a first location and a second location transparently to a user at the first location" (emphasis added), as recited in claim 26. Moreover, *Pfaffenberger* does not remedy the deficiencies of *Kiuchi* at least because *Pfaffenberger* also fails to disclose that a domain name service system is configured to enable establishment of a secure communication link between a first location and a second location transparently to a user at the first location, as recited in claim 27. Nor does the Office Action or Request rely on *Pfaffenberger* for such disclosure. Accordingly, the rejection of claim 27 in view of *Kiuchi* and *Pfaffenberger* should be withdrawn and the claim should be confirmed.

k. Dependent Claims 2-4, 6, 7, 11, 14-16, 18, 19, 22, 25, 28-30, 33, 34, 37-40, 42, 43, 46, 49-54, and 57-59

Remaining claims 2-4, 6, 7, 11, 14-16, 18, 19, 22, 25, 28-30, 33, 34, 37-40, 42, 43, 46, 49-54, and 57-59 depend from one of independent claims 1 and 36 and include all of their features. Thus, the combination of *Kiuchi* and *Pfaffenberger* does not render obvious any of these claims for at least

Several events also demonstrate praise for the inventions in the '504 patent by those in the field. As discussed above, SAIC invested a disproportionately large percentage of its internal resources in the technology. (*Id.* ¶ 17.) SafeNet, Microsoft, and Aastra have all licensed the technology. (*Id.*; Ex. A-5 at 1.) A study done by CSMG praised the inventions. (Short Decl. in control no. 95/001,788 ¶ 17.) Jim Rutt at Network Solutions, which was eventually acquired by Verisign, praised and expressed significant interest in the technology and would have invested but for a change in circumstances at his company. (*Id.*) This evidence showing that the claimed inventions met a long-felt need, succeeded where others have failed, have been commercially successful, were contrary to the accepted wisdom at the time of the invention, were met by skepticism by those skilled in the art, and were praised by others in the field, rebuts any finding that the claimed inventions would have been obvious.

IV. Conclusion

For at least these reasons, VirnetX requests reconsideration and withdrawal of the rejections in the Office Action and confirmation of the patentability of all of the claims of the '504 patent.

VirnetX notes that the Request, Order, and Office Action contain a number of assertions and allegations concerning the disclosure, claims, and cited references. VirnetX does not subscribe to any assertion or allegation in the Request, Order, and Office Action regardless of whether it is addressed specifically herein.

Please grant any extension of time and charge any required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: June 1, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508